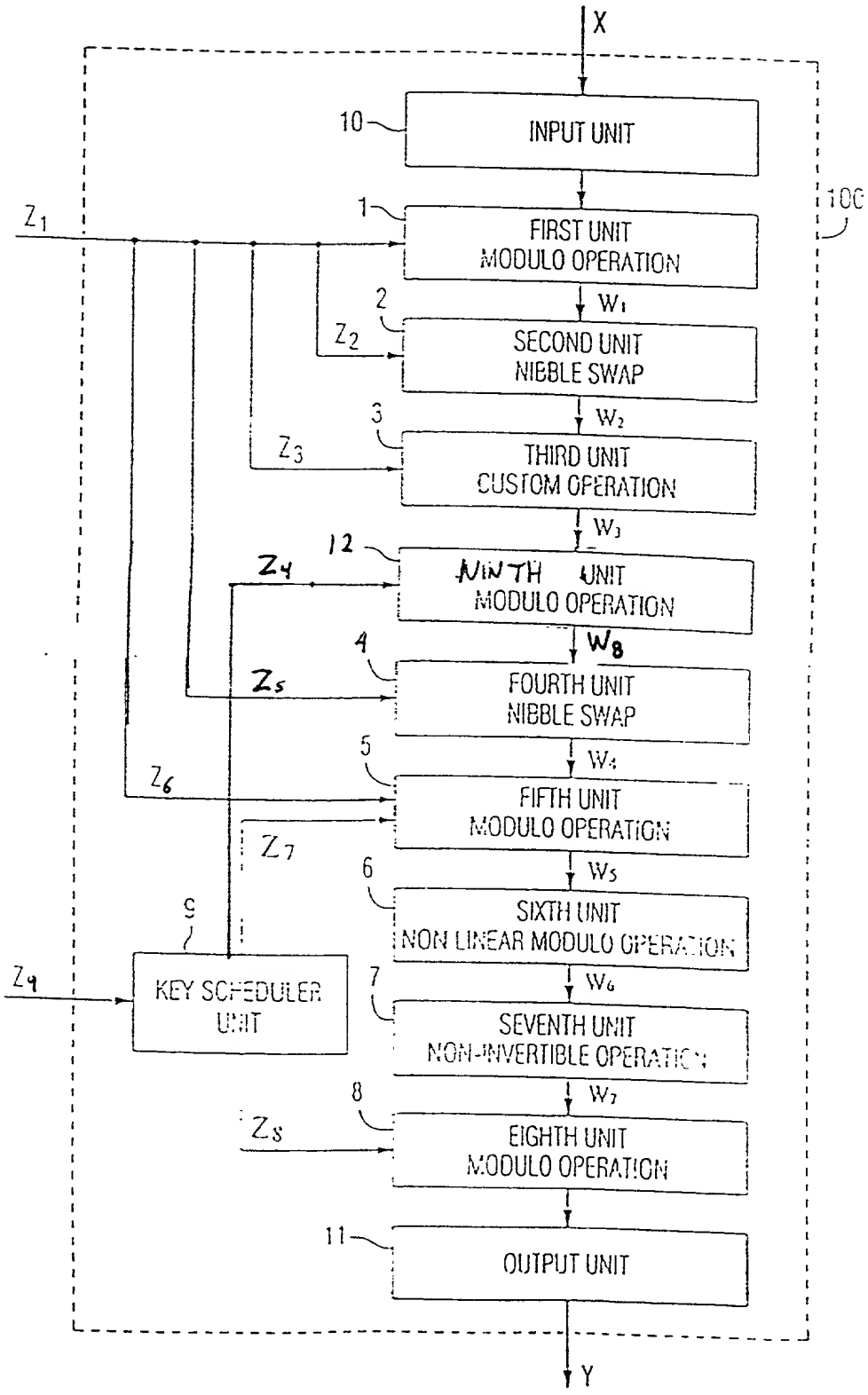
X
10
INPUT UNIT
100
1
FIRST UNIT
MODULO OPERATION
Z1
W1
2
SECOND UNIT
NIBBLE SWAP
Z2
W2
3
THIRD UNIT
CUSTOM OPERATION
Z3
W3
12
NINTH UNIT
MODULO OPERATION
Z4
W8
4
FOURTH UNIT
NIBBLE SWAP
Z5
W4
5
FIFTH UNIT
MODULO OPERATION
Z6
Z7
W5
6
SIXTH UNIT
NON LINEAR MODULO OPERATION
W6
7
SEVENTH UNIT
NON-INVERTIBLE OPERATION
W7
8
EIGHTH UNIT
MODULO OPERATION
Z8
9
KEY SCHEDULER
UNIT
Z9
11
OUTPUT UNIT
Y

FIG. 1

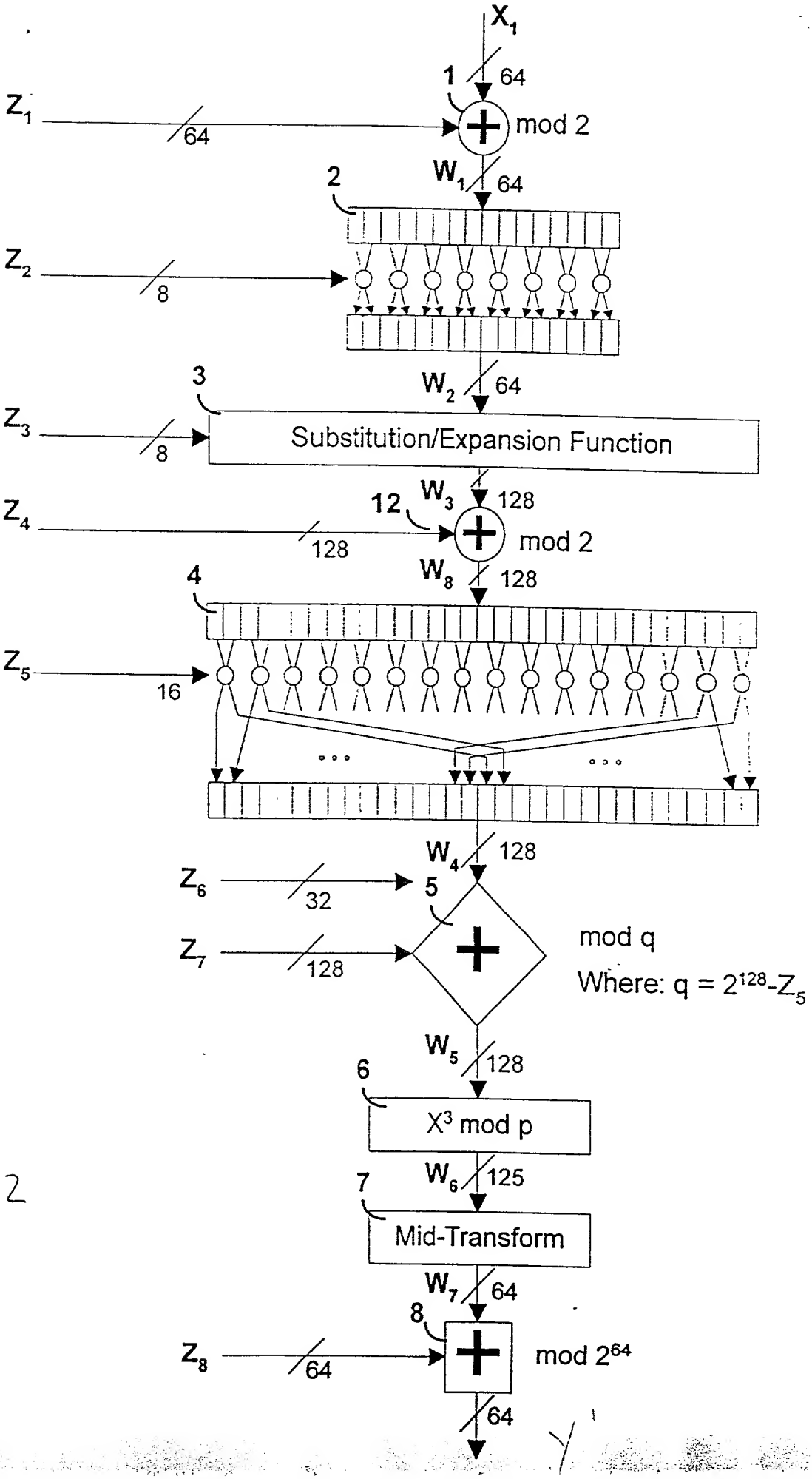
X1
1
64
Z1
64
mod 2
W1
64
2
Z2
8
W2
64
3
Z3
8
Substitution/Expansion Function
W3
128
12
Z4
128
mod 2
W8
128
4
Z5
16
W4
128
Z6
32
5
Z7
128
mod q
Where: q = 2128-Z5
W5
128
6
X3 mod p
W6
125
7
Mid-Transform
W7
64
8
Z8
64
mod 264
64

FIGURE 2

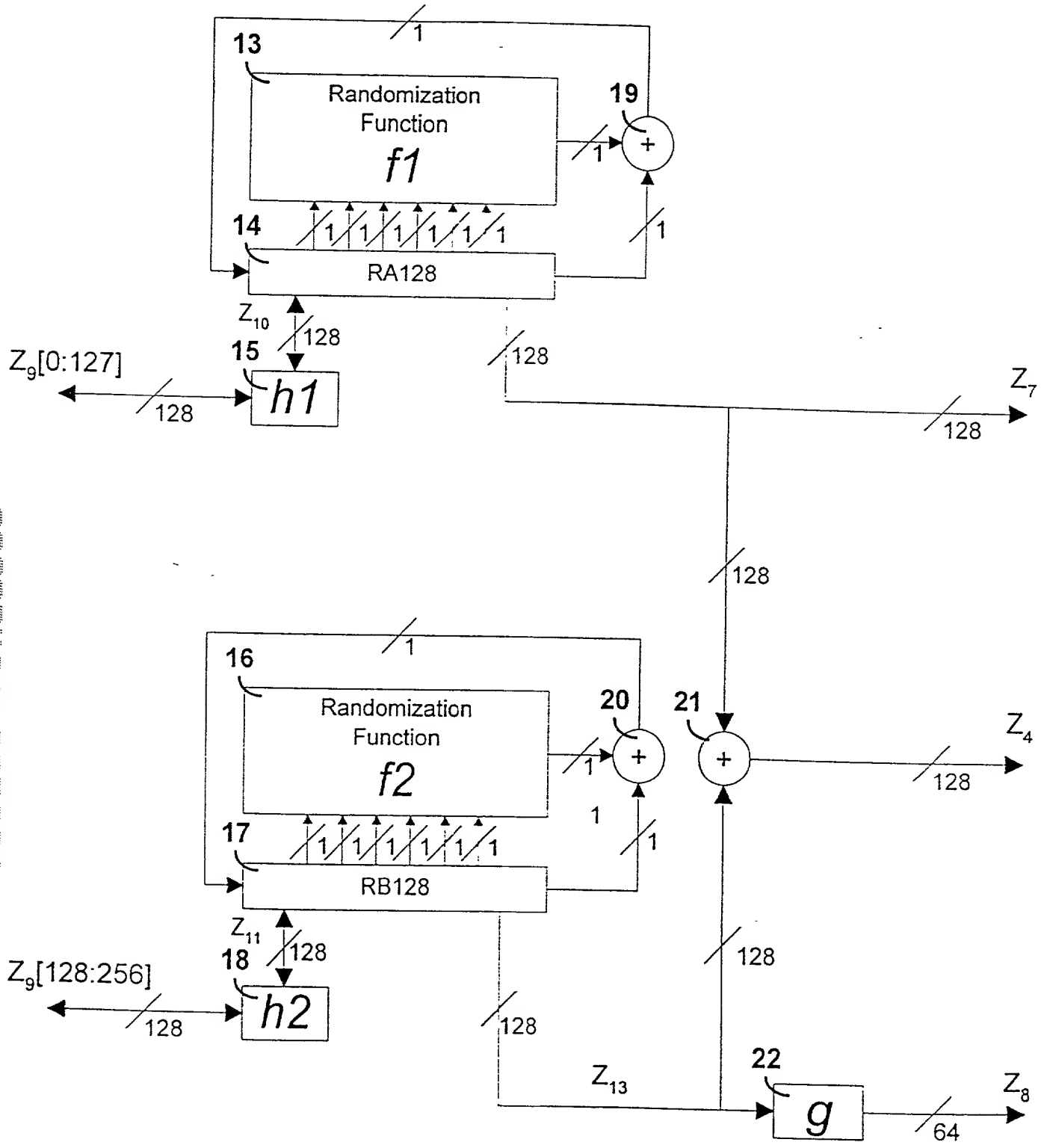
13
Randomization Function
f1
19
14
RA128
Z_{10}
15
h1
$Z_g[0:127]$
Z_7
16
Randomization Function
f2
20
21
Z_4
17
RB128
Z_{11}
18
h2
$Z_g[128:256]$
Z_{13}
22
g
Z_8
64
128

FIGURE 3

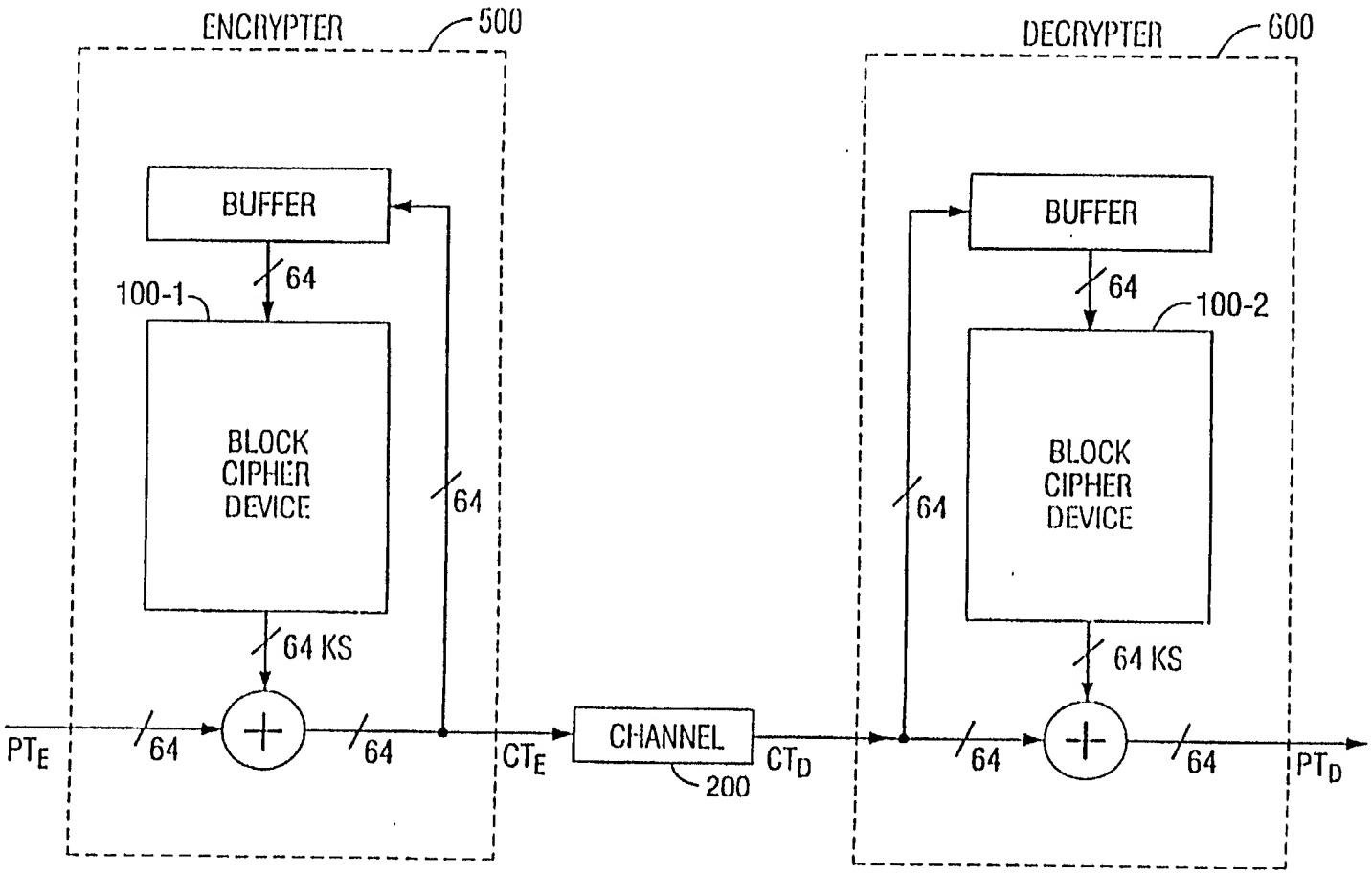

FIG. 4

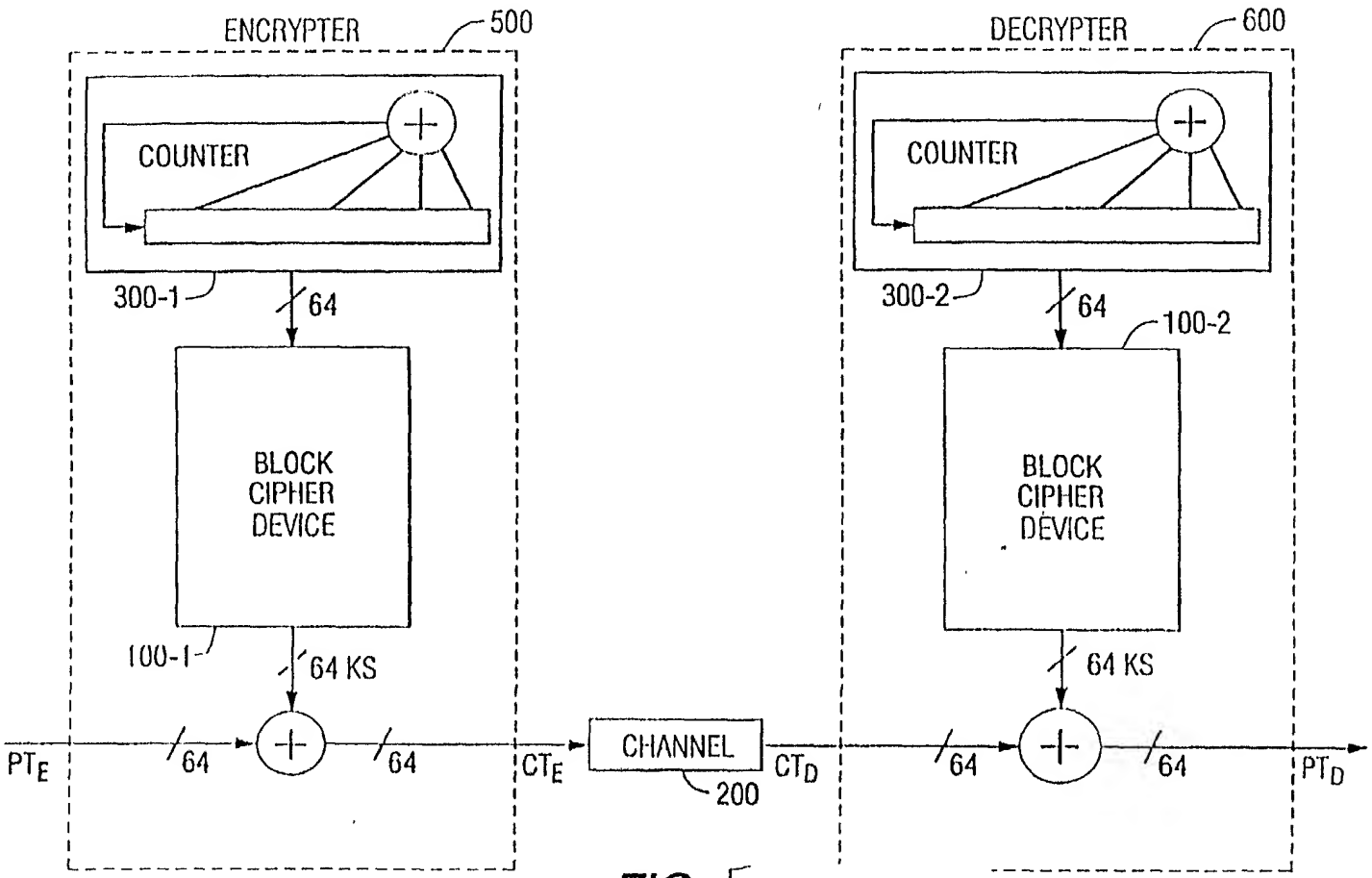

FIG. 5

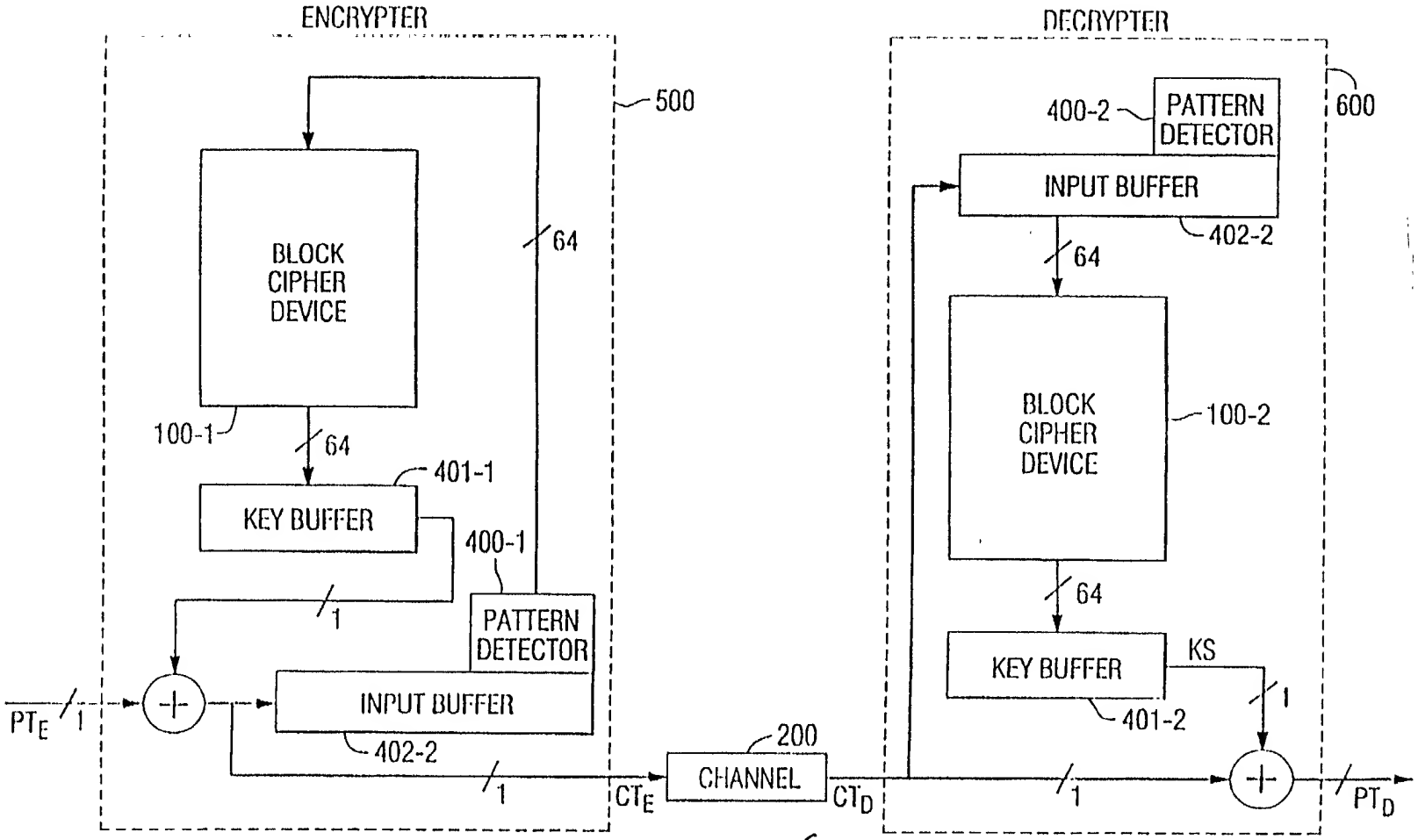

FIG. 6